

Les études et les métiers de la sécurité informatique

Florent Autréau – Clément Pernet – **Laurent Mounier**

Forum des Masters et des Licences Professionnelles – 3 mars 2022

CyberSécurité : une menace bien réelle ...

Augmentation constante des usages de l'informatique

Modification des pratiques :

objets connectés, cloud, systèmes autonomes, etc.

→ accroissement de la **surface d'attaque**

Coût économique majeur :

3 trillions \$ (un trillion = 10^{18}) en 2015,
6 trillions en 2020, ...



Des cibles multiples :

- ~ particuliers
- ~ entreprises
- ~ banques
- ~ administrations
- ~ sites de production
- ~ états
- ~ etc.

Des conséquences graves :

- ~ vol de données
- ~ destruction de données
- ~ paralysie de systèmes informatiques
- ~ destruction d'outils de production
- ~ malversations financières
- ~ atteintes à la vie privée
- ~ etc.

... et des réponses à plusieurs niveaux

- **agences gouvernementales** : ANSSI
- **normes et règlements** : RGPD, Critères Communs
- **plans d'investissements** : plan cybersecurité, grand défi cybersecurité
- **coopération internationale** : recensement de vulnérabilités, systèmes de chiffrement

- **prise de conscience** des éditeurs de logiciels, des autres entreprises/administration (PSSI)
- essor d'**entreprises spécialisées** (conseil, audit, analyse, outils, etc.)

- effort de **recherche** important : académique et industriel
- techniques et outils pour la protection des systèmes informatiques
- intégration dans les **cursus de formation** en informatique ...

CyberSécurité : un large spectre de compétences

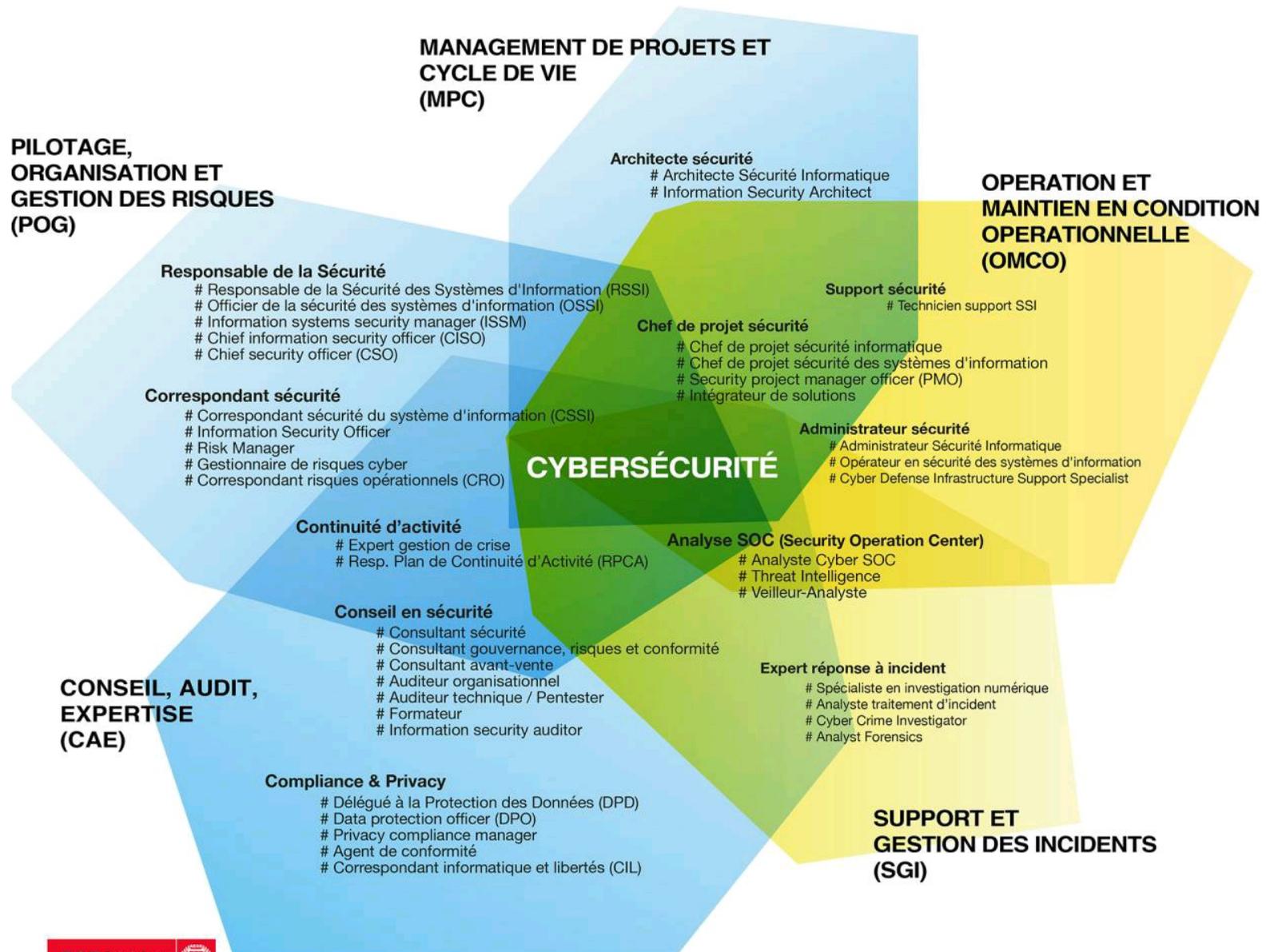
De nombreuses facettes ... :

- réseaux
- cryptographie
- développement logiciel
- langages, compilation
- architectures matérielles
- droit, informatique légale
- etc.

... qui couvrent de multiples domaines :

- informatique
- mathématiques appliquées
- mathématiques pures
- électronique, automatique
- droit, sciences sociales
- etc.

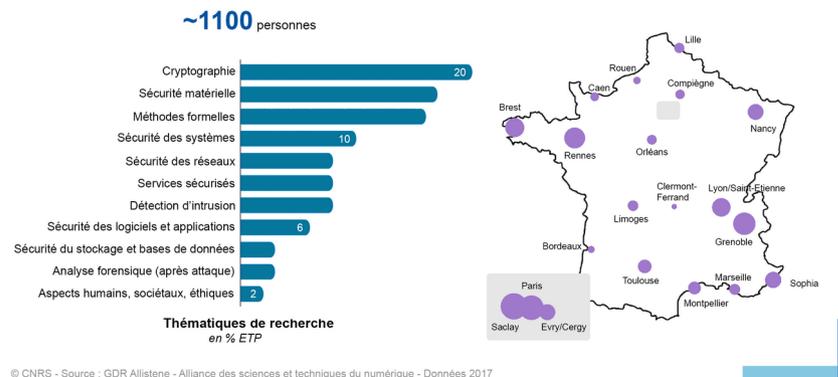
Exemples de métiers en cybersécurité



La cybersécurité à Grenoble

La cybersécurité, une communauté restreinte mais dynamique

Répartition des 102 équipes travaillant sur la cybersécurité en France



Une forte communauté académique :

UGA, INRIA, Grenoble INP, CEA

structurée autour du **CDP Cybersecurity Institute**



Cybersecurity Institute

Université Grenoble Alpes

De nombreuses **entreprises** : ST Microelectronics, Schneider, ...

Une **conférence annuelle** :



Les formations au niveau Master (UGA, G-INP)



M2
CSIL



M2 CySec



M2 RIE

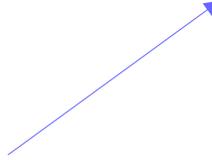


Spécialité
Réseaux et Télécom

M1 RIE

M1 Scientifique à majeure informatique (> 60 ECTS)
(Info, MoSiG, MSIAM, Maths Générales, etc.)

Licence Scientifique
(INF, MIN, MAI, Maths, etc.)



M2 CSIL : Cybersécurité et Informatique Légale

Éléments clés :

- formation en **alternance**, 50 % des enseignements effectués par des intervenants extérieurs
- enseignement en français, évaluation par « projets » (contrôle continu intégral)
- promotions : ≤ 16 étudiants

Programme :

- architectures de sécurité, administration de réseaux sécurisés
- ingénierie cryptographiques et protocoles
- audit et analyse de risques
- sécurité des composants et des logiciels et applications multimédias
 - (OS, systèmes embarqués, systèmes industriels)
- informatique légale et aspects législatifs
 - (politiques de la cybersécurité, investigation numérique, protection de la vie privée)
- apprentissage et projet en entreprise

Principaux débouchés :

Ingénieur/consultant spécialiste en cybersécurité et informatique légale

Responsable sécurité des systèmes d'Information (RSSI), etc .

Eléments clés :

- formation M2 *classique* (1 semestre de cours, 1 semestre de stage en entreprise/laboratoire)
- enseignement en **anglais** (~ 50 % de l'effectif non francophone)
- promotion : ~ 40 étudiants

Programme :

- software security, secure programming
- security architectures : network, system, cybersecurity of industrial IT
- cryptographic engineering, protocols and security models, data privacy,
- threat and risk analysis, IT security audit and norms
- physical security : Embedded, Smart Card, Quantum & Biometrics
- advanced cryptology or advanced Security
- internship

Principaux débouchés :

- ingénieur expert en cybersécurité (R&D, conseils, audit, etc.)
- thèse de doctorat (recherche en milieu académique ou industriel)

Eléments clés :

- formation en **alternance** (2 jours en enseignement, 3 jours en entreprise)
- Admission en **1ère ou 2ème année**

Programme (M2) :

- systèmes et applications réparties
- ingénierie de la sécurité
- sécurité des réseaux
- réseaux sans fils et cellulaires
- management et organisation des entreprises
- anglais
- projet en entreprise

Principaux débouchés :

- ingénieur expert en réseaux informatiques
- (architecture, sécurité, administration et maintenance d'applications en réseaux)

Quelques liens ...

- **M2 Cybersécurité et Informatique Légale (CSIL)**

<https://im2ag.univ-grenoble-alpes.fr/parcours-cybersecurite-et-informatique-legale/>

- **M2 Cybersecurity (CySec)**

<https://im2ag.univ-grenoble-alpes.fr/parcours-cybersecurity-2e-annee/>

- **Master Réseaux Informatique d'Entreprise (RIE)**

<https://ensimag.grenoble-inp.fr/fr/formation/rie>

Questions ?